CLAIMS

1. A method of identifying a user participating in a network communication session comprising the steps of:

creating a master database having a first table with a first plurality of cells for a set of binary keys, a second plurality of cells for a plurality of key pointers, and third plurality of cells for markers identifying an instance of an application;

creating a second table in the master database with a first plurality of cells for information related to eligible users and a second plurality of cells for user-associated tokens;

creating an application to be accessed by eligible users over a communications network;

associating the master database with the application to be accessed by the eligible users identified in a second table of the master database;

generating a plurality of binary key pointers and a plurality of binary keys of a predetermined length and associating each binary pointer with a unique one of the binary keys;

associating the key pointers with a first instance of the application;

entering information relating to the eligible users for the first instance into the first plurality of cells in the second table;

generating a plurality of tokens;

associating each eligible user with a unique one of the tokens from the plurality of tokens by placing the associated token in a position in the second plurality of cells in the second table corresponding to the eligible user in the first plurality of cells in the second table;

encrypting each user-associated token with a randomly selected one of the plurality of binary keys;

prepending each encrypted token with the key pointer associated with the binary key used to encrypt the token;

providing the combined key pointer and encrypted token to the associated eligible user;

receiving the combined key pointer and encrypted token returned by a user through the communications network;

finding the key pointer in the second plurality of cells of the first table;

retrieving the corresponding binary key from the first plurality of cells in the first table if the key pointer is found in the second plurality of cells of the first table and the key pointer received is not marked as disabled;

decrypting the encrypted token sent by the user using the retrieved binary key from the first plurality of cells of the first table if the binary key is found in the first plurality of cells in the first table and the binary key is not marked as disabled;

retrieving the corresponding information relating to the eligible user from the first plurality of cells in the second table if the token is found in the second plurality of cells of the second table and the token is not marked as disabled; and

using this information to give the eligible user access to the corresponding instance of the application.

2. The method of claim 1 further comprising the step of encoding the combined key pointer and encrypted token to conform to the protocols of the communications network.

3. The method of claim 1 wherein the binary key pointers are cryptographically random.

4. The method of claim 1 wherein the tokens are cryptographically random.

5. The method of claim 1 wherein each of the tokens contains a nested checksum.

6. The method of claim 1 further comprising the step of denying access to the user if the key pointer received cannot be found in the second plurality of cells of the first table or the key pointer received is marked as disabled.

7. The method of claim 1 further comprising the step of denying access if the binary key is not found in the first plurality of cells of the first table or the binary key is marked as disabled.

8. The method of claim 5 further comprising the step of verifying that the nested checksum in the decrypted token contains the values corresponding to the algorithm by which it was generated; and

9. The method of claim 8 further comprising the step of denying access to the user if the values contained in the nested checksum are not correct.

10. The method of claim 8 further comprising the step of finding the decrypted token in the second plurality of cells of the second table if the nested checksum is correct.

11. The method of claim 8 further comprising the step of denying access to the user if the token is not found in the second plurality of cells in the second table or the token is marked as disabled.

12. A method of identifying a user participating in a network communication session comprising the steps of:

creating a master database having a first table with a first plurality of cells for a set of binary keys, a second plurality of cells for a plurality of key pointers, and third plurality of cells for markers identifying an instance of an application;

creating a second table in the master database with a first plurality of cells for information related to eligible users and a second plurality of cells for user-associated tokens;

creating an application to be accessed by eligible users over a communications network;

associating the master database with the application to be accessed by the eligible users identified in a second table of the master database;

generating a plurality of binary key pointers and a plurality of binary keys of a predetermined length and associating each binary pointer with a unique one of the binary keys;

associating the key pointers with a first instance of the application;

entering information relating to the eligible users for the first instance into the first plurality of cells in the second table;

generating a plurality of tokens;

associating each eligible user with a unique one of the tokens from the plurality of tokens by placing the associated token in a position in the second plurality of cells in the second table corresponding to the eligible user in the first plurality of cells in the second table;

encrypting each user-associated token with a randomly selected one of the plurality of binary keys; and

prepending each encrypted token with the key pointer associated with the binary key used to encrypt the token.

13. The method of claim 12 further comprising the step of encoding the combined key pointer and encrypted token to conform to the protocols of the communications network.

14. The method of claim 12 wherein the binary key pointers are cryptographically random.

15. The method of claim 12 herein the tokens are cryptographically random.

16. The method of claim 12 herein each of the tokens contains a nested checksum.

17. The method of claim 12 further comprising the steps of:

providing the combined key pointer and encrypted token to the associated eligible user;

receiving the combined key pointer and encrypted token returned by a user through the communications network;

finding the key pointer in the second plurality of cells of the first table;

retrieving the corresponding binary key from the first plurality of cells in the first table if the key pointer is found in the second plurality of cells of the first table and the key pointer received is not marked as disabled;

decrypting the encrypted token sent by the user using the retrieved binary key from the first plurality of cells of the first table if the binary key is found in the first plurality of cells in the first table and the binary key is not marked as disabled;

retrieving the corresponding information relating to the eligible user from the first plurality of cells in the second table if the token is found in

the second plurality of cells of the second table and the token is not marked as disabled; and

using this information to give the eligible user access to the corresponding instance of the application.

18. The method of claim 17 further comprising the step of denying access to the user if the key pointer received cannot be found in the second plurality of cells of the first table or the key pointer received is marked as disabled.

19. The method of claim 17 further comprising the step of denying access if the binary key is not found in the first plurality of cells of the first table or the binary key is marked as disabled.

20. The method of claim 17 further comprising the step of verifying that the nested checksum in the decrypted token contains the values corresponding to the algorithm by which it was generated; and

21. The method of claim 20 further comprising the step of denying access to the user if the values contained in the nested checksum are not correct.

22. The method of claim 21 further comprising the step of finding the decrypted token in the second plurality of cells of the second table if the nested checksum is correct.

23. The method of claim 22 further comprising the step of denying access to the user if the token is not found in the second plurality of cells in the second table or the token is marked as disabled.